SpyWolf

Project Audit

Project:

MoonPad

May 11, 2022

Overview

This audit has been prepared for **MoonPad** to review the main aspects of the project to help investors make an informative decision in the research process.

You will find a a summarized review of the following main key points:

- Contract's source code
- Project and team
- Website
- Social media & online presence

NOTE: We ONLY consider a project safe if they receive our "Certificate of Trust" NFT. This report only points out any potential red flags found in our analysis. Always do your own research before investing in a project.

Smart Contract Review

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities

- Assessing the codebase to ensure compliance with current best practices and industry standards.

- Ensuring contract logic meets the specifications and intentions of the client.

- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.

- Thorough line-by-line manual review of the entire codebase by industry experts.

"The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal"
- SpyWolf Team

Smart Contract Summary

Contract Name	MoonPadToken
Ticker	MoonPad
Contract	0xCeB765c234C14BE577b8E13b4CdCDa6aD47b6ad6
Network	Binance smart chain
Language	Solidity
Tax	**Buy: 6%** **Sell: 10%**
Total Supply	6,000,000,000
Status	Launched

Current stats

Burn	No burnt tokens
LP Address	No liquidity added yet
Liquidity	No liquidity added yet
MaxTxAmount	50,000

Issues Checking Status

Design Logic	**Passed ✓**
Compiler warnings.	**Passed ✓**
Private user data leaks	**Passed ✓**
Timestamp dependence	**Passed ✓**
Integer Overflow and Underflow	**Passed ✓**
Race conditions and Reentrancy. Cross-function race conditions	**Passed ✓**
Possible delays in data delivery	**Passed ✓**
Oracle calls	**Passed ✓**
Front running	**Passed ✓**
DoS with Revert	**Passed ✓**
DoS with block gas limit	**Passed ✓**
Methods execution permissions	**Passed ✓**
Economy model	**Passed ✓**
The impact of the exchange rate on the logic	**Passed ✓**
Malicious Event log	**Passed ✓**
Scoping and Declarations	**Passed ✓**
Uninitialized storage pointers	**Passed ✓**
Arithmetic accuracy	**Passed ✓**
Cross-function race conditions	**Passed ✓**
Safe Zeppelin module	**Passed ✓**
Fallback function security	**Passed ✓**

Featured Wallets

Owner address	0x21F3A03eD4CBa9ac80c2C109e7dbaF493440De22
*Auto liquidity receiver	0x0000000000000000000000000000000000000000
*Marketing fee receiver	0x0000000000000000000000000000000000000000
*Staking fee receiver	0x0000000000000000000000000000000000000000
*Team fee receiver	0x0000000000000000000000000000000000000000
LP address	Liquidity not added yet

*Owner can change this address in future

Top 3 Unlocked Wallets

Wallet 1 (100%)	Same as owner

Tokens are not distributed yet

Security Threats

Owner can change max transaction limit, but can't lower it lower than 0.1% of total supply. The current default limit is 0.001% of total supply.

```
function setTxLimit(uint256 amount) external onlyOwner {
    require(amount >= _totalSupply / 1000, "Limit too low");
    _maxTxAmount = amount;
}
```

⚠️**Owner can blacklist address, making it impossible to sell.**

```
function setIsBlacklisted(address adr, bool state) external onlyOwner {
    require(adr != address(0), "Cannot blacklist zero address");
    require(adr != address(owner()), "Cannot blacklist owner address");
    isBlacklisted[adr] = state;
}
```

⚠️**Owner can change buy/sell fees up to 100%.**

```
function setBuyFees(
    uint256 _liquidityFee,uint256 _stakingFee, uint256 _marketingFee,
    uint256 _burnFee,uint256 _feeDenominator
) external onlyOwner {
    buyLiquidityFee = _liquidityFee;
    buyStakingFee = _stakingFee;
    buyMarketingFee = _marketingFee;
    buyBurnFee = _burnFee;
    buyFeeDenominator = _feeDenominator;
}

function setSellFees(
    uint256 _liquidityFee,uint256 _stakingFee,uint256 _marketingFee,
    uint256 _burnFee,uint256 _teamFee, uint256 _feeDenominator
) external onlyOwner {
    sellLiquidityFee = _liquidityFee;
    sellStakingFee = _stakingFee;
    sellMarketingFee = _marketingFee;
    sellBurnFee = _burnFee;
    sellTeamFee = _teamFee;
    sellFeeDenominator = _feeDenominator;
}
```

Security Threats

Buy fees works fine.
When sell fees are above 6% for each input field or above than 10% in 3 input fields (more than 31% combined for all types), selling fails.
If the fees are below 31% percent, selling works.
Tokens deducted from both buys/sells are distributed to the assigned addresses correctly.

⚠️ **If the "liquifyAmount" is changed from the "setLiquify()" function, the contract loses its ability to swap the liquidity tokens fee. Tokens are deducted from transfers, but instead of swapping and sent to the correct address, they just accumulate in the contract.**

With the default settings there is no problem with the automatic swap and send of the

```
function setLiquify(bool enabled, uint256 amount) external onlyOwner {
    require(amount <= 1000 * (10**_decimals));
    liquifyEnabled = enabled;
    liquifyAmount = amount;
}
```

Tokenomics

Current state:

According to their telegram chat:

There is currently migration to a new contract going on, because of problems with the old one. Since the liquidity is locked, the team collects all available tokens from users to sell them and drain the current liquidity pool. They then will pair the liquidity with the new contract. All current holders will receive 1:1 airdrop, even if they don't send their tokens to the team.

SpyWolf

MoonPad
Project & Team Review

According to their whitepaper:

MoonPad will be a decentralized presale and IDO platform based on the Binance Smart Chain and also going to be launched on the PulseChain.

There will be staking pool where users can stake their tokens to receive rewards.

In order to participate in IDO's, users will be required to stake their $MoonPad tokens for at least 24 hours.

Moonpad will be a tiered Launchpad. The more tokens users hold, the bigger allocation they will get in IDOs.

Users will be able to unstake their tokens at any time - there is fee of 3% for unstaking.

Team:

MoonPad
Project & Team Review

Team:
https://spywolf.network/assets/kyc/2022/may/Team_KYC_moonpad_
0xCeB765c234C14BE577b8E13b4CdCDa6aD47b6ad6.png

Website Analysis

URL: https://moonpad.live/

- **Design:** Smooth single page design, appropriate color scheme.

- **Content:** Informative, no grammar mistakes.

- **Whitepaper:** Well written, explanatory.

- **Roadmap:** Goals set at 4 phases with time frames.

- **Mobile-friendly?** Yes

- **Technical:** SSL certificate present. General SEO check passed.

moonpad.live
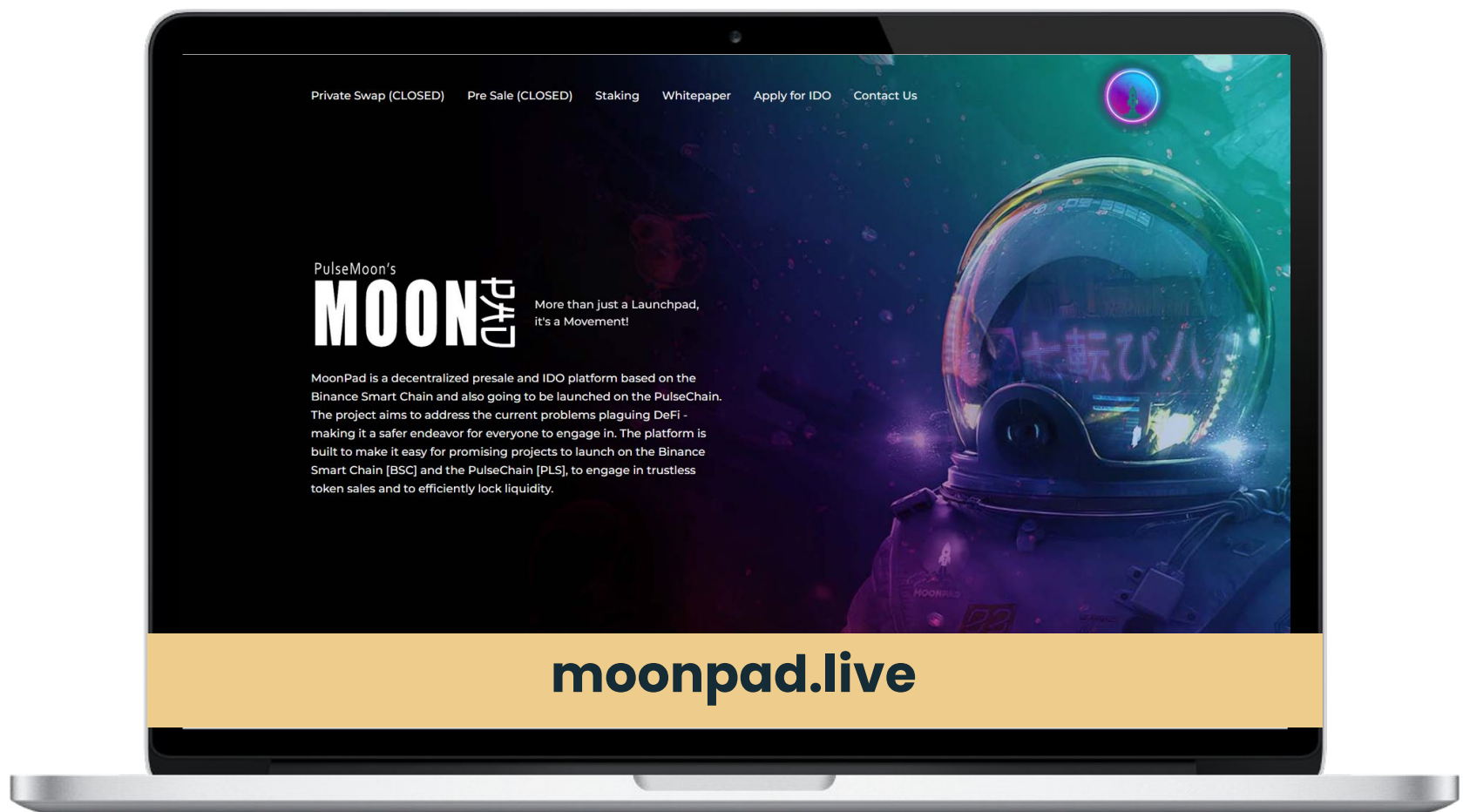
Social Media & Online Presence

Telegram

https://t.me/MoonPadOfficial

- 1 727 members
- Active members
- Active mods

Twitter

https://twitter.com/pulsemoon2
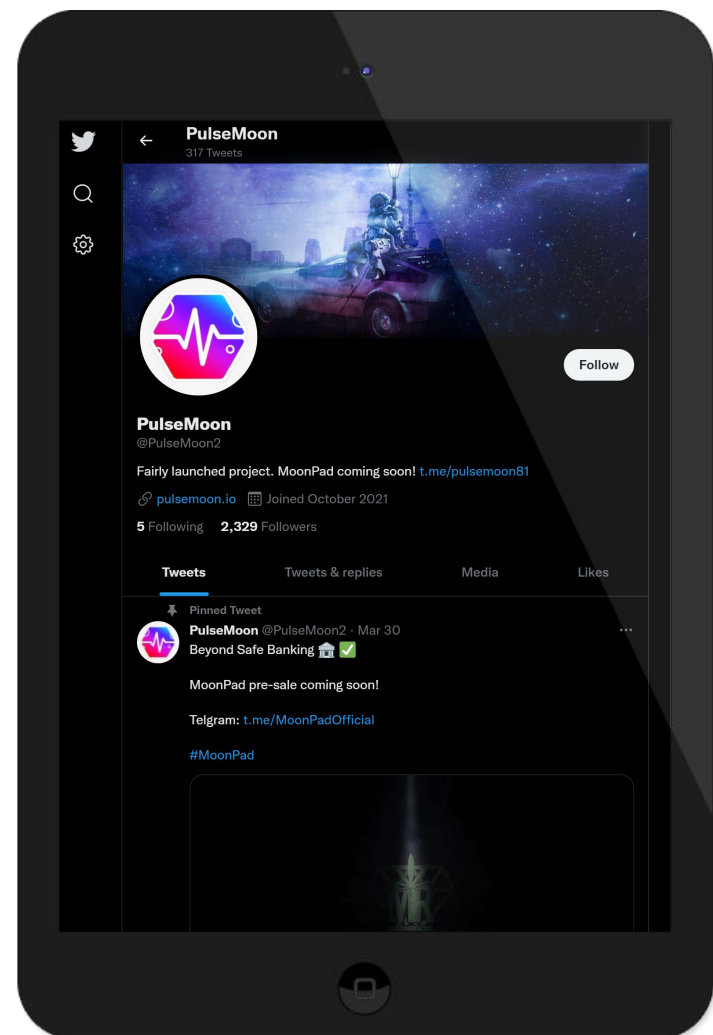
- 2 327 Followers
- Active

About SpyWolf

SpyWolf is a team of crypto security experts that have been performing full audits for projects for the past months in order to ensure safety on the crypto space. Our goal is to help eliminate monetary fraud through our auditing services and utility token, $SPY.

▶ Website: SpyWolf.co

▶ Portal: SpyWolf.network

▶ Telegram: @SpyWolfNework

▶ Twitter: Twitter.com/SpyWolfNetwork
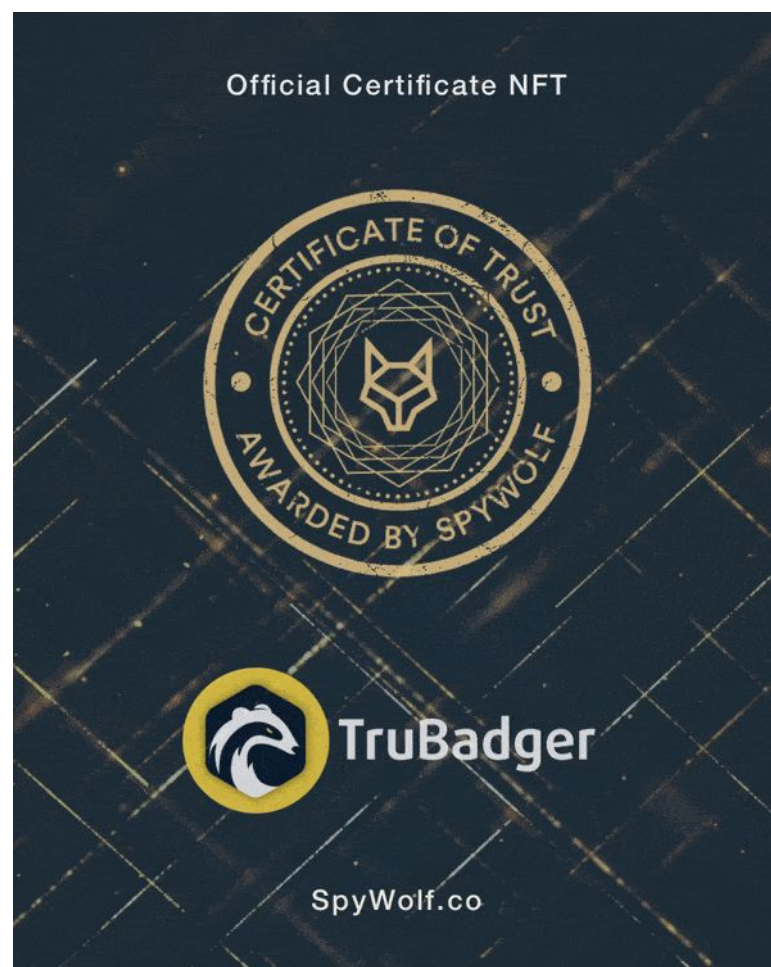
(Sample Certificate NFT for those who pass audit)

If you are interested in finding out more about our audits and Certificate of Trust NFTs, reach out to contact@spywolf.co.

SpyWolf

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.